AF
IFW

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of: Jay C. Chen Serial No.: 09/456,794 Filed: December 8, 1999 For: A CRYPTOGRAPHIC SYSTEM AND METHOD FOR ELECTRONIC TRANSACTION	Customer Number:33401 Confirmation Number: 6924 Group Art Unit: 2137 Examiner: P. Callahan

CERTIFICATE OF MAILING (37 C.F.R. § 1.8(a))

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail under 37 CFR 1.8(a) in an envelope addressed to, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on Dec. 20, 2005.

Anita Chou

APPELLANT'S BRIEF

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria. VA 22313-1450

Commissioner:

Appellant hereby files its brief on appeal under 37 CFR § 1.192. A Notice of Appeal was filed in the above-reference application on October 20, 2005.

1. REAL PARTY IN INTEREST

The real party in interest is Jay C. Chen.

2. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

3. STATUS OF CLAIMS

Claims 82-116 are the subject of this appeal.

Claims 82-84, 86, 88-90, 92-94, 96, 97, 103, 104, and 106-116 stand rejected under 35 USC §103(a) as unpatentable over *Ginzboorg et al.* (U.S. Patent No. 6,240,091) in view of *Schneier,* Applied Cryptography, 2nd Ed, Oct. 1995.

Claim 85 stands rejected under 35 USC §103(a) as unpatentable over *Ginzboorg et al.* in view of *Schneier* and further in view of *Walker et al.* (US Patent No. 6,263,438).

Claims 87, 91, 95, 98-102, and 105 stand rejected under 35 USC §103(a) as unpatentable over *Ginzboorg et al.* in view of *Schneier* and further in view of Official Notice.

4. STATUS OF AMENDMENTS

There are no pending amendments in the present application.

5. SUMMARY OF INVENTION

Two common types of cryptographic systems that have been developed to increase security for electronic transactions are secret key based systems and public/private key based systems. A secret key based system (on an open network such as the Internet) is less flexible in terms of key distribution and key management and is more vulnerable to malicious attack. Public/private key systems have their own disadvantages, one of which, is the daunting task of authenticating transaction parties to one another.

The present invention, as defined in the claims reproduced in the attached Appendix, is directed towards various methods to perform secure communications between a member and a service provider. These methods provide an improvement over conventional approaches by providing security without the need for a secret key or a trusted third party. As a result, the need for digital certificates and for separate, trusted certificate authorities has been eliminated. In one embodiment of the cryptographic system, the member initiates communications with a service provider by sending a key exchange request message. The key exchange request message includes the member's public key, and is encrypted, at least in part, with the service provider's public key stored on an electronic or smart card of the member. The service provider, in response to the key exchange request message, generates a session key to be used to conduct a transaction between the two.

In another embodiment, the service provider and two members are involved in the key exchange request and response. FIG. 2 of the present application depicts this embodiment and is described at page 12, line 10 – page 14, line 15. In particular, a first member **102** uses a public key of the service provider **106** to encrypt a message having the member's public key (arrow **1**)

that is sent to the second member **104**. The service provider's public key is included within an electronic card of the first member **102**. Second member **104** combines its own message (having his own public key) with the received message, and digitally signs at least a portion of it, and sends the combined key exchange message (arrow **2**) to the service provider **106**. In response to receiving the combined message, the service provider **106** verifies the signed message using the included public key of the second member and generates a first session key and a second session key. The service provider generates a key exchange response message for the first member **102** that includes the first session key and is digitally signed by the service provider **106**. Also, the service provider **106** generates a key exchange response message for the second member **104** that includes the second session key and is digitally signed by the service provider **106**. The key response messages are combined into a combined key exchange response message and sent (arrow **3**) to the second member **104**. Because the second member **104** also has an electronic card with the service provider's public key, the second member **104** is able to separate the combined response message to recover the key exchange response message for the second member and then forward (arrow **4**) the key exchange response message for the first member to the first member **102**. With the session keys exchanged, the members may conduct a secure transaction using the session keys for encryption (arrows **5 – 10**).

6. ISSUES

The issues presented for review on appeal are:

1. Whether claims 82-84, 86, 88-90, 92-94, 96, 97, 103, 104, and 106-116 are unpatentable under 35 USC §103(a) over *Ginzboorg et al.* (U.S. Patent No. 6,240,091) in view of *Schneier,* Applied Cryptography, 2nd Ed, Oct. 1995.

2. Whether claims 85 are unpatentable under 35 USC §103(a) over *Ginzboorg et al.* in view of *Schneier* and further in view of *Walker et al.* (US Patent No. 6,263,438).

3. Whether claims 87, 91, 95, 98-102, and 105 are unpatentable under 35 USC §103(a) over *Ginzboorg et al.* in view of *Schneier* and further in view of Official Notice.

7. GROUPING OF CLAIMS

Claims 82 and 83 stand or fall together.

Each of claim 85, 98, 114, and 115 stands or falls on its own.

Claims 84, 86-91, and 95 stand or fall as a group.

Claims 92-94 stand or fall as a group.

Claims 96, 97, and 99-102 stand or fall as a group.

Claims 103, 105, 107-109, and 112 stand or fall as a group.

Claims 104 and 110 stand or fall together.

Claims 106 and 111 stand or fall together.

Claims 113 and 116 stand or fall together.

8. ARGUMENT

A. The rejection of claims 82 and 83 is improper because a prima facie case of obviousness has not been established.

1) One of ordinary skill would not have been realistically motivated to modify *Ginzboorg et al.* to include portions of the Woo-Lam and EKE protocols.

As noted earlier, claim 82 stands rejected under 35 USC §103(a) as unpatentable over *Ginzboorg et al.* in view of *Schneier*. In particular, the Examiner asserts that *Ginzboorg et al.* teaches an electronic card having a public key of a service provider. The Examiner further asserts that *Schneier* teaches substantially all the remaining claim limitations.

Appellant submits that considering the rejection as merely the combination of two references does not correctly describe the present circumstances. The text by *Schneier* is more than simply a single, coherent reference; it consists of hundreds of pages of different cryptography-related protocols. Each such protocol having an applicable environment in which it operates and having a respective purpose. In the present rejections, three or four different protocols are combined in various ways – the Woo-Lam protocol, the Otway-Rees protocol, the EKE protocol and a fourth, generic protocol. Admittedly, all these protocols may be found described in a single reference (i.e., *Schneier*); however, Appellant urges that these different protocols should not be treated as simply a consistent, coherent teaching of a single cryptographic system.

In particular, the Woo-Lam protocol requires that a third party exists that is trusted by the two parties that are going to perform a transaction. Furthermore, the protocol uses public key/private key encrypted messages (asymmetric encryption) to generate a session key. The Otway-Rees protocol also involves a trusted third party but only relies on symmetrically encrypted messages. In contrast, the EKE protocol uses a two-party (instead of three) communication model but requires that a common secret password be pre-arranged between the

two parties. These differences are some of the reasons that the Woo-Lam protocol has eight steps, the Otway-Rees protocol has five steps, and the EKE protocol has six steps; wherein for each of the protocols, every step relies on the specific previous sequence of steps and the particular information contained and exchanged therein. Thus, each of the protocols is a series of inter-related, specific exchanges occurring in a particular order. Appellant urges that, as a general principle, one of ordinary skill would not have been realistically motivated to separate these disparate protocols into their component parts and then selectively re-combine the parts, sometimes out-of-order, in the hope of achieving the presently claimed invention.

Separate from the general argument just provided about combining selective pieces of different protocols, Appellant disagrees with the specific combination of teachings proffered by the Examiner in rejecting claim 82. The system of *Ginzboorg et al.* involves a network service provider that includes a charging server that a customer contacts to initiate service. The charging server is able to authenticate a customer's message that is signed with the customer's private key using its database of stored public keys. The Woo-Lam and the EKE protocols are two different protocols used under two different circumstances that allow two parties to mutually authenticate each other's identities.

According to the Patent Office, the "desire to verify digital signature" in *Ginzboorg et al.* provides the motivation for combining *Ginzboorg et al.* with the Woo-Lam protocol and the EKE protocol. Appellant respectfully disagrees. *Ginzboorg*'s system discloses the use of a subscriber database at the service provider site that contains the public keys from all the subscribers. For example, in column 8, lines 66-67 and column 9, lines 1-3, *Ginzboorg et al.* state that after having received the signed contract CDR, the charging server of the service provider verifies the signature by using a known method in order to authenticate the CDR. "For this purpose, the charging server receives from its subscriber database the public key for the customer in question (arrow C in Fig 5)." Thus, it is clear that the service provider and its public-key database of *Ginzboorg et al.* already provides the ability to verify digital signatures from its subscribers without the need for an additional key exchange protocol and therefore has no reason to work with Woo-Lam or the EKE protocols for this purpose.

The Examiner, in the Final Office Action (page 2), indicates that Appellant's argument against the combination is not convincing because *Ginzboorg et al.* desires "high-speed data transmission" and that the "[u]se of Woo-Lam and EKE would offer the advantage of higher

speed as the majority of the transaction processing would take place at the subscriber." Appellant believes that this rationale is flawed for at least two reasons:

1) The portion of the patent referred to by the Examiner relates to transmission rates of a physical media. The need for selecting media with high transmission rates is unrelated to the processing speed of performing a transaction. Instead the transmission rate of the media is important because of the multimedia services that are in demand (see column 1, lines 19-23). This need for an appropriate physical network medium to handle large amounts of data is not a basis for realistically motivating one of ordinary skill to modify the way digital signatures are verified in *Ginzboorg et al.*

2) Secondly, the hypothetical changes to *Ginzboorg et al.* would likely have the opposite effect and slow transaction processing time. As presently configured, *Ginzboorg et al.* requires the exchange of one message from a user to the server in order for the server to be able to verify the user's digital signature. Replacing such a verification method with a multi-step protocol would detrimentally affect the speed of the transaction. The Woo-Lam protocol requires the transmission of seven different messages, some of which are highly complex (see for example, steps 5 and 6). Each such message introduces a transit time between the sender and the receiver. Each such message requires encrypting before sending and decrypting subsequent to receiving. In view of these additional processing demands at both the sender and receiver and the cumulative effect of transmission delay times, Appellant urges that one of ordinary skill would not have been realistically motivated to modify *Ginzboorg et al.* to include the Woo-Lam protocol in the interest of improving "speed".

In addition to *Ginzboorg et al.* and Woo-Lam, the Examiner combines them with the EKE protocol to reject claim 82. As noted earlier, the EKE protocol is a two-party protocol that requires a pre-arranged secret password between the two parties while, in contrast, the Woo-Lam protocol is a three-party protocol that does not require a pre-arranged secret password between all the participants. In view of these differences, Appellant urges that one of ordinary skill would not have been realistically motivated to selectively choose one step of the EKE protocol with which to modify the Woo-Lam protocol, as suggested by the Examiner.

In view of the above arguments, Appellant urges that a prima facie case of obviousness has not been established because the Examiner has not provided a cogent explanation of why one

of ordinary skill would have been realistically motivated to modify the system of *Ginzboorg et al.* to specifically incorporate the Woo-Lam protocol and the EKE protocol. Accordingly, Appellant respectfully requests that the Examiner's rejection of claim 82 be reversed.

2) The combination of *Ginzboorg et al.* with portions of the Woo-Lam and EKE protocols does not yield the claimed invention.

As noted earlier, claim 82 stands rejected under 35 USC §103(a) as unpatentable over *Ginzboorg et al.* in view of *Schneier*. In particular, the Examiner asserts that *Ginzboorg et al.* teaches an electronic card having a public key of a service provider. The Examiner further asserts that *Schneier* teaches substantially all the remaining claim limitations. Claim 82 recites, in part,

formatting a key exchange request message at a member, the key exchange request message having a public key of the member, and at least a portion of the key exchange request message being encrypted using the service provider's public key from the electronic card;

sending the key exchange request message from the member to the service provider;

The Examiner asserts that step 3 of the Woo-Lam protocol, from *Schneier*, teaches this claim limitation. In step 3 of Woo-Lam, the message that is generated is sent from Alice to Bob; it is apparently this message that the Examiner considers the same as the "key exchange request message" recited in the claim. Thus, in accordance with the claim language, Alice is the "member" from the claim and Bob is the "service provider" from the claim. To remain consistent with this reading of the Woo-Lam protocol, the claim requires that message in step 3 of the Woo-Lam protocol have a public key of Alice.

However, in direct contrast to this requirement, the message from step 3 of the Woo-Lam protocol does **not** have the public key of Alice. Instead this message does not include any public key but, instead, includes a random number and Alice's name.

The claim continues by reciting:

generating a session key exclusively at the service provider in response to the key exchange request message;

The Examiner asserts that step 5 of the Woo-Lam protocol teaches the above claim limitations. To remain consistent with the application of Woo-Lam (step 3) described earlier, these claim limitations would require that the session key be exclusively generated at Bob (the service provider) and be generated in response to the key exchange message. Appellant urges that there are factual inconsistencies between the disclosed operation of step 5 of the Woo-Lam protocol and the limitations of the claim. In particular, Step 5 of the Woo-Lam protocol involves a random session key that is generated by Trent. The claim recites that the service provider (Bob) generates the session key, while step 5 of the Woo-Lam protocol teaches that Trent generates the random session key. This difference highlights that Woo-Lam requires a trusted third party be available to permit effective operation of its protocol which is in direct contrast to *Ginzboorg et al.* which relies on the service provider's own database of public keys to authenticate a customer.

Because of the reasons discussed above, Appellant submits that even if the teachings of *Ginzboorg et al.*, the Woo-Lam protocol, and the EKE protocol were combined, the combination would not yield the claimed invention. Accordingly, Appellant respectfully requests that the Examiner's rejection of claim 82 be reversed.

Claims 83 - 95 are dependent from claim 82 and, therefore, are also patentable for at least the same reasons set forth above and the rejection of these claims should also be reversed. There are a number of additional reasons for patentability addressed below.

B. The rejection of claims 84, 86-91, and 95 is improper because combination of *Ginzboorg et al.* with portions of the Woo-Lam and EKE protocols does not yield the claimed invention.

Claim 84 recites, in part,:

(a) formatting by the member a transaction request message using the session key, the transaction request message including a digital signature of the member, and sending the transaction request message to the service provider; and

(b) formatting at the service provider, a transaction response message for the member using the session key, the transaction response including a digital signature of the service provider, and sending the transaction response message to the member.

In rejecting this claim, the Examiner asserts that both limitations (a) and (b) are taught by Steps 6-8 of the Woo-Lam protocol. Appellant respectfully disagrees with this characterization of the Woo-Lam protocol. Firstly, in steps 6 and 7 of Woo-Lam, the parties (Alice and Bob) have yet to be convinced of each other's identity. Accordingly, the exchange in these steps is still part of authenticating each other and should not be considered as a transaction message (request or response) as required by the claims.

Additionally, in Woo-Lam, step 7 involves the message from the member (Alice) to the service provider (Bob). This message merely consists of Bob's random number and does not "use the session key" nor include Alice's digital signature as required by limitation (a).

Furthermore, step 6 involves the message from the service provide (Bob) to the member (Alice). According to the protocol, this message includes Trent's digital signature but does not include Bob's (the service provider) digital signature as required by limitation (b).

Because of the reasons discussed above, Appellant submits that even if the teachings of *Ginzboorg et al.*, the Woo-Lam protocol, and the EKE protocol were combined, the combination would not yield the claimed invention. Accordingly, Appellant respectfully requests that the Examiner's rejection of claim 84 be reversed. For the same reason, the rejection of dependent claims 86-91, and 95 should also be reversed.

C. The rejection of claim 85 is improper because a prima facie case of obviousness has not been established.

1) <u>One of ordinary skill would not have been realistically motivated to modify *Ginzboorg et al.* to include portions of *Walker et al.* the Woo-Lam and EKE protocols.</u>

The Examiner asserts that the combination of references applied to claim 82, teaches substantially all the limitations of this claim but does not disclose the specific limitations of claim 85. The Examiner relies on *Walker et al.* for disclosing encryption of financial transaction data by a symmetric key and contends that one would be motivated to make the combination because "this would increase the utility and hence the marketability of the system."

The language of claim 85 specifically requires at least two features:

(a) that it be the "transaction request message" that include the recited content; and

(b) that the recited content include a "transaction amount".

Returning to the rejection of claim 84 for a moment, the Examiner asserted that the transaction request message is sent from the member (Alice) to the service provider (Bob) and corresponds to step 7 of the Woo-Lam protocol. At this point in the Woo-Lam protocol Alice is certain of Bob's identity but Bob is not yet convinced of her's; it is premature to exchange transaction data at this stage of Woo-Lam. Accordingly, regardless of the disclosure of *Walker et al.*, Appellant respectfully submits that one of ordinary skill would not have been realistically motivated to modify the message in step 7 of Woo-Lam to include transaction-specific information such as account information, transaction amount, etc. because all parties are not yet certain of the identity of other parties.

In view of the above arguments, Appellant urges that a prima facie case of obviousness has not been established because the Examiner has not provided a cogent explanation of why one of ordinary skill would have been realistically motivated to modify a message in the Woo-Lam protocol to specifically incorporate the transaction data purportedly disclosed by *Walker et al.* Accordingly, Appellant respectfully requests that the Examiner's rejection of claim 85 be reversed.

2) The combination of *Ginzboorg et al.* with *Walker et al.* portions of the Woo-Lam and EKE protocols does not yield the claimed invention.

Even if the references could be combined as suggested by the Examiner, Appellant urges that the combination would not yield the claimed invention. In particular, the claim requires that the transaction request message include a "transaction amount". Contrary to the Examiner's characterization, the system of *Walker et al.* fails to disclose or suggest such a feature. *Walker*'s system relates to secure document timestamping (see column 3, lines 60-62). That system is unconcerned with a transaction amount and does not disclose or suggest encrypting such information symmetrically or asymmetrically.

For at least this reason, Appellant submits that even if the teachings of *Ginzboorg et al.*, *Walker et al.*, the Woo-Lam protocol, and the EKE protocol were combined, the combination would not yield the claimed invention. Accordingly, Appellant respectfully requests that the Examiner's rejection of claim 85 be reversed.

D. The rejection of claims 92 - 94 is improper because One of ordinary skill would not have been realistically motivated to modify *Ginzboorg et al.* to include portions of page 51 of *Schneier,* the Woo-Lam protocol and the EKE protocol.

The specific limitations of claim 92 relate to a transaction acknowledgement message and the way that it is formulated and encrypted. The Examiner asserts that an exchange protocol on page 51 of *Schneier* discloses the specific features of claim 92 and, thus, in combination with the earlier references teaches all the features recited in claim 92.

Claim 92 depends from claim 84 which was rejected in view of *Ginzboorg et al.* combined with the Woo-Lam protocol and the EKE protocol. Returning to the system of *Ginzboorg et al.*, the service provider already includes a database that stores the public key for the users which can be used to verify digital signatures. In contrast to this, is the Woo-Lam protocol which requires a multi-step three-party protocol involving a trusted third party to allow users to authenticate themselves. Furthermore, in Woo-Lam it is the trusted third party that generates the session key for later use. Appellant has previously argued that one of ordinary skill would not have been realistically motivated to pick-and-choose portions of these two systems and combine them together.

In rejecting claim 92, the Examiner has introduced yet another protocol that is different than Woo-Lam and the EKE protocol and asserts that it would have been obvious to modify Woo-Lam to incorporate the features of this other protocol in order to provide increased security. The Examiner appears to contend that this additional protocol teaches generating a transaction acknowledgement message that is digitally signed by the member and sent to the service provider.

In this latest protocol, a previously performed key-exchange protocol is <u>not</u> needed before exchanging a transaction message between the two parties, although that is the express purpose of the Woo-Lam protocol. Furthermore, in this latest protocol, the participation of a trusted third party in exchanging messages is eliminated, although, in direct contrast, Woo-Lam requires participation of such a third party.

Appellant recognizes that these different systems all include cryptography-related protocols and that (according to long-standing convention) the parties are typically named Alice, Bob, Carol, Dave, Trent, etc and involve various encryption steps performed by the various

parties. However, Appellant respectfully asserts that "increased security" is not a realistic motivation as to why one of ordinary skill would have specifically modified the Woo-Lam protocol to include steps from such a dramatically different protocol as the one at page 51 of *Schneier*. The assertion of "increased security" is an illusion because the digital signatures used in the latest protocol are for protection against a specific vulnerability to "man-in-the-middle" attacks at step 4 of the protocol.

A man-in-the-middle attack is when an attacker can modify messages without either party knowing the link has been compromised. Looking carefully at the stage in the protocol that suggests a digital signature (i.e., step 4), an attacker can intercept Alice's message without Alice being aware that it happened. As far as Alice knows, her message, M, was received by Bob. Although the attacker cannot read the message, M, the attacker can generate his own random session key and encrypt it with Bob's public key and generate his own message and encrypt in with his generated session key. At this stage, nothing in the message from the attacker relies on knowledge that is unique to Alice. Accordingly, if Bob was sent the attacker's message, then Bob would be unable to detect that this message came from someone other than Alice, unless the protocol was enhanced to require Alice's digital signature at step 4.

However, if Woo-Lam is used as a key exchange protocol, the session key is ultimately used by the parties to securely conduct a transaction. In other words, both parties use a secret key (the session key) that is known only to them to conduct a transaction. Thus, the particular man-in-the-middle vulnerability for transaction messages that would be solved by including simple digital signatures has already been addressed and eliminated in Woo-Lam.

Appellant urges that "increased security" would not have resulted from the hypothetical combination of *Ginzboorg et al.* and the Woo-Lam protocol to with portions of yet another protocol related to preventing man-in-the-middle attacks. In view of the above arguments, Appellant urges that a prima facie case of obviousness has not been established because the Examiner has not provided a cogent explanation of why one of ordinary skill would have been realistically motivated to modify *Ginzboorg et al.* and the Woo-Lam protocol in view of the protocol on page 51 of *Schneier*. Accordingly, Appellant respectfully requests that the Examiner's rejection of claim 92 be reversed. For the same reason, the rejection of dependent claims 93 and 94 should also be reversed.

E. The rejection of claims 96, 97, and 99-102 is improper because a prima facie case of obviousness has not been established.

1) One of ordinary skill would not have been realistically motivated to modify *Ginzboorg et al.* to include portions of the Woo-Lam and EKE protocols.

Appellant has provided, with respect to claim 82, arguments why one of ordinary skill would not have been motivated to combine the references as suggested by the Examiner. In view of these arguments, Appellant urges that a prima facie case of obviousness has not been established because the Examiner has not provided a cogent explanation of why one of ordinary skill would have been realistically motivated to modify the system of *Ginzboorg et al.* to specifically incorporate the Woo-Lam protocol and the EKE protocol. Accordingly, Appellant respectfully requests that the Examiner's rejection of independent claim 96, and its dependent claims, be reversed.

2) The combination of *Ginzboorg et al.* with portions of the Woo-Lam and EKE protocols does not yield the claimed invention.

Claim 96 recites:

generating a member challenge by a member;
encrypting by the member the member challenge using the service provider's public key from the electronic card to generate a first cryptogram;

The Examiner asserts that Woo-Lam step 4 discloses these limitations. According to Woo-Lam step 4, a message is generated and encrypted by Bob using Trent's public key. Thus, unlike the rejection of claim 82, where Alice was the member and Bob was the service provider, the interpretation of Woo-Lam, with respect to claim 96, would mean that the claimed member is "Bob" (the one generating and encrypting) and the claimed service provider is "Trent" (the one who's public key is used). Step 4 of the Woo-Lam protocol does not involve Bob generating his own challenge. Even if the random number from Alice, R_A, is considered a challenge, then it is Alice's challenge which would not teach or suggest Bob (the member) generating a challenge as required by the claim.

If, however, the claim interpretation stated with respect to the rejection of claim 82, is maintained such that step 3 of Woo-Lam is interpreted as reading on these limitations, the Appellant respectfully asserts that the same reasons previously argued with respect to claim 83

are relevant and that the combination of references does not teach or suggest these recited limitations of claim 96.

Claim 96 continues later on by reciting:

generating exclusively by the service provider a session key;
encrypting by the service provider the service provider challenge and the session key using the member's public key to generate a second cryptogram;

The Examiner asserts that this is disclosed by steps 3 through 5 of the EKE protocol. In the EKE protocol, the session key and the service provider challenge are sent as two separate messages. First, in step 2, the service provider (Bob in EKE) generates and sends the session key to the member (Alice for EKE). Then separately, in step 4, the service provider (Bob) generates and sends a challenge. Thus, the steps of the EKE protocol do not teach or suggest encrypting the service provider challenge and the session key to generate a second cryptogram, as required by the claim. Additionally, according to the EKE protocol, the encryption of the service provider challenge is performed using the session key instead of using the member's public key, as required by the claim.

Claim 96 continues by reciting:

formatting by the service provider a key exchange response message including the second cryptogram and a response to the member challenge;
signing digitally by the service provider the key exchange response message;
sending the digitally signed key exchange response message to the member;

The Examiner asserts that these claim features are also disclosed by steps 3 through 5 of the EKE protocol. According to the claim, the key exchange response message identified in these claim features has at least the following features:

a) includes the second cryptogram (i.e., the service provider challenge and the session key both encrypted using the member's public key),

b) includes the second cryptogram and a response to the member (Alice's) challenge,

c) an be signed digitally by the service provider.

Appellant urges that no such message is sent to Alice (the member) in any steps of the EKE protocol.

Claim 96 finishes by reciting

encrypting by the member a member response for the service provider challenge using the session key to generate a third cryptogram;

attaching the third cryptogram to a transaction message going from the member to the service provider;

signing digitally by the member the transaction message going from the member to the service provider; and

sending the transaction message from the member to the service provider.

The Examiner asserts that these features are disclosed by steps 5 and 6 of the EKE protocol. According to step 5 of the EKE protocol, Alice generates a message that includes the member response to the service provider challenge and is encrypted using the session key. This is the message that is sent from Alice (the member) to Bob (the service provider) which the Examiner apparently believe disclose the third cryptogram of the claim. However, the claim also requires that the recited third cryptogram be attached to a transaction message. The EKE protocol does not teach or suggest this feature and simply does not even contemplate a transaction message combined with the message Alice sends Bob. Additionally, the claim requires that the transaction message be digitally signed by the member (Alice). This feature is also not taught or suggested by the EKE protocol.

For at least these reasons, Appellant submits that even if the teachings of *Ginzboorg et al.*, the Woo-Lam protocol, and the EKE protocol were combined, the combination would not yield the claimed invention. Accordingly, Appellant respectfully requests that the Examiner's rejection of claim 96 be reversed along with the rejection of dependent claims 97-102.

F. The rejection of claim 98 is improper because combination of *Ginzboorg et al.* with portions of the Woo-Lam and EKE protocols does not yield the claimed invention.

Claim 98 recites that the key exchange request message include the member's public key encrypted with the service provider's public key. The Examiner asserts that step 4 of the Woo-Lam protocol and step 1 of the EKE protocol disclose this feature. In step 4 of Woo-Lam, the

message that is sent does not include the member's public key and, thus, also does not include the member's public key encrypted with the service provider's public key. In step 1 of the EKE protocol, the message is not encrypted with the service provider's (Bob's for EKE) public key. Thus, neither the EKE protocol nor the Woo-Lam protocol teach or suggest the feature recited in claim 98. For at least these reasons, Appellant submits that even if the teachings of *Ginzboorg et al.*, the Woo-Lam protocol, and the EKE protocol were combined, the combination would not yield the claimed invention. Accordingly, Appellant respectfully requests that the Examiner's rejection of claim 98 be reversed.

G. The rejection of claims 103, 105, 107, 108, 109, and 112 is improper because a prima facie case of obviousness has not been established.

1) The combination of *Ginzboorg et al.* with portions of the Woo-Lam and Otway-Rees protocols does not yield the claimed invention.

Without much explanation, the Examiner asserts that whatever limitations of claim 103 that are not found in claim 82 are taught by the combination of *Ginzboorg et al.* with portions of the Woo-Lam and Otway-Rees protocols. Appellant is uncertain how the two different protocols can be read on the claims in a consistent manner. For example, when Woo-Lam was applied to claim 82, the member was Alice and the service provider was Bob and Trent was not ignored. However, when applying the Otway-Rees protocol, a more consistent application would be to have Alice and Bob be the first and second members, respectively, and Trent be the service provider. Even overlooking that the different protocols cannot be simultaneously and consistently applied to the language of claim 103, the combination of the two protocols (in conjunction with *Ginzboorg et al.*) do not yield the claimed invention.

Claim 103 requires that the first member send a first key exchange request to a second member and that the second member send a combination key exchange request message to the service provider.

sending the first key exchange request message from the first member to a second member;

combining at a second member, a second member key exchange request message with the first member's key exchange request message and sending the combined key exchange request message, signed by the second member, to a service provider;

Because the Otway-Rees protocol relies on a respective secret symmetric key between Alice and Trent and Bob and Trent, each of Alice and Bob send their own request messages to Trent (i.e., steps 1 and 2 of the Otway-Rees protocol). Thus, the combination of protocols proposed by the Examiner does not teach or suggest the combined key exchange request message sent by only the second member to the service provider, as recited in the claim.

According to the claim, the service provider generates both a first session key and a second session key.

generating a first session key exclusively by the service provider in response to the first key exchange request message;
generating a second session key exclusively by the service provider in response to the second key exchange request message;

In the Otway-Rees protocol, Trent generates one session key that is shared with both Alice and Bob. Thus, the combination of protocols suggested by the Examiner does not teach or suggest the generating of the second session key.

According to the claim, the encryption involving the response messages is performed by the service provider digitally signing the appropriate message.

formatting a key exchange response message at the service provider including a first session key for the first member, signing the response message, formatting a key exchange response message including the second session key for the second member, combining the key exchange response messages into a combined key exchange response message, signing the combined key exchange response message, and sending the combined key exchange response message to the second member

In the Otway Rees protocol, the first response message is encrypted with the first member's shared key and the second response message is encrypted with the second member's shared key. Thus, the combination of protocols suggested by the Examiner does not teach or suggest the digital signing by the service provider required by the claims.

For at least these reasons, Appellant submits that even if the teachings of *Ginzboorg et al.*, the Woo-Lam protocol, and the Otway-Rees protocol were combined, the combination would not yield the claimed invention. Accordingly, Appellant respectfully requests that the Examiner's rejection of claim 103, and its dependent claims, be reversed.

Claim 109 recites similar claim limitations to those of claim 103 except that an intermediate member, who may not being a participating member, might be involved in the exchange. Thus, for at least the reasons provided with respect to claim 103, Appellant respectfully requests that the Examiner's rejection of claims 109 – 112 be reversed.

2) One of ordinary skill would not have been realistically motivated to modify *Ginzboorg et al.* to include portions of the Woo-Lam and Otway-Rees protocols.

As mentioned, the Examiner rejects claim 103 in view *Ginzboorg et al.* and the Woo-Lam protocol as applied to claim 82 further in view of the Otway-Rees protocol. For the same reasons presented earlier with respect to claim 82, Appellant urges that a prima facie case of obviousness has not been established with respect to claim 103 because the Examiner has not provided a cogent explanation of why one of ordinary skill would have been realistically motivated to modify the system of *Ginzboorg et al.* to specifically incorporate the Woo-Lam protocol. Accordingly, Appellant respectfully requests that the Examiner's rejection of claim 103, and its dependent claims, be reversed.

Additionally, the Otway-Rees protocol has now been added to the combination of references on which the rejection is based. The Otway-Rees protocol is relied on for disclosing all those features of claim 103 that are not found in claim 82. Appellant believes that these features of claim 103 include all the claim limitations except for the "formatting a first key exchange request message ... using the service provider's public key from the electronic card." The Examiner contends that the addition of the Otway-Rees protocol satisfies a desire to prevent "replay attacks". That is, an attack where an attacker captures a valid message between a user and a server and then presents it to the server at some later time.

Appellant urges that the Examiner has not met the burden of establishing a prima facie case of obviousness because there is no explanation of how the Woo-Lam protocol suffers from a "replay attack" vulnerability and, therefore, how inclusion of the Otway-Rees protocol would eliminate this vulnerability. Without the Woo-Lam protocol needing protection from a "replay attack", there is no motivation to incorporate additional steps to prevent such an attack. Therefore, Appellant urges that a prima facie case of obviousness has not been established because the Examiner has not provided a cogent explanation of why one of ordinary skill would

have been realistically motivated to modify the system of *Ginzboorg et al.* combined with the Woo-Lam protocol to specifically incorporate only selected portions of the Otway-Rees protocol. Accordingly, Appellant respectfully requests that the Examiner's rejection of claim 103, and its dependent claims, be reversed.

Claim 109 recites similar claim limitations to those of claim 103 except that an intermediate member, who may not being a participating member, might be involved in the exchange. Thus, for at least the reasons provided with respect to claim 103, Appellant respectfully requests that the Examiner's rejection of claims 109 – 112 also be reversed.

H. The rejection of claims 104 and 110 is improper because combination of *Ginzboorg et al.* with portions of the Woo-Lam and Otway-Rees protocols does not yield the claimed invention.

The limitations recited in claim 104 are many and detailed. However, in general, they relate to a transaction occurring between the first and second member which is in contrast to claim 103 which related to the key exchange request and response messages involving the two members. Appellants urge that even if the teachings of *Ginzboorg et al.*, the Woo-Lam protocol, and the Otway-Rees protocol were combined, the combination would not yield the claimed invention.

Although having vastly different pre-conditions and assumptions, both the Woo-Lam protocol and the Otway-Rees protocol share the common attribute that they are performed before a transaction between two parties can take place. The reason is that before these protocols are performed, the user's are not certain of each other's identity. Therefore, Appellant submits that the Otway-Rees protocol or the Woo-Lam protocol, either considered individually or in combination, do not teach or suggest anything resembling a transaction request or transaction response message as recited in claim 104. For at least these reasons, Appellant submits that even if the teachings of *Ginzboorg et al.*, the Woo-Lam protocol, and the Otway-Rees protocol were combined, the combination would not yield the claimed invention. Accordingly, Appellant respectfully requests that the Examiner's rejection of claims 104 - 108 be reversed.

Claim 110 recites similar claim limitations to those of claim 104. Thus, for at least the reasons provided with respect to claim 104, the combination of references would not yield the

claimed invention of claim 110. Accordingly, Appellant respectfully requests that the Examiner's rejection of claim 110 be reversed.

I. The rejection of claim 106 and 111 is improper because combination of *Ginzboorg et al.* with portions of the Woo-Lam and Otway-Rees protocols does not yield the claimed invention.

In the Otway-Rees protocol, Trent generates one session key that is shared with both Alice and Bob. However, according to the claim, the service provider generates both a first session key and a second session key, that are different. Thus, the combination of protocols suggested by the Examiner does not teach or suggest the generating of the second, different session key, as required by the claim.

Claim 111 recites similar claim limitations to those of claim 104. Thus, for at least the reasons provided with respect to claim 106, the combination of references would not yield the claimed invention of claim 111. Accordingly, Appellant respectfully requests that the Examiner's rejection of claim 111 be reversed.

J. The rejection of claim 113 and 116 is improper because a prima facie case of obviousness has not been established.

1) <u>One of ordinary skill would not have been realistically motivated to modify *Ginzboorg et al.* to include portions of the Woo-Lam and Otway-Rees protocols.</u>

For at least the reasons already provided with respect to claim 103, Appellant submits that one of ordinary skill would not have been motivated to combine the references as suggested by the Examiner. Therefore, Appellant urges that a prima facie case of obviousness has not been established because the Examiner has not provided a cogent explanation of why one of ordinary skill would have been realistically motivated to modify the system of *Ginzboorg et al.* combined with the Woo-Lam protocol to specifically incorporate only selected portions of the Otway-Rees protocol. Accordingly, Appellant respectfully requests that the Examiner's rejection of claim 113, and its dependent claims, be reversed.

2) The combination of *Ginzboorg et al.* with portions of the Woo-Lam and Otway-Rees protocols does not yield the claimed invention.

In addition to the reasons already provided with respect to claim 103, Appellant submits that claim 113 includes additional features not taught or suggested by the applied combination of references. In particular, unlike previous claims, claim 113 does not simply recite that there is a first member but that their are a plurality of first members that each send a respective key exchange request message to the second member. Furthermore, the claim recites generating respective session keys for each of the plurality of first members and sending these keys to the first members. These features are not taught or suggested by the combination of the Woo-Lam and Otway-Rees protocols which disclose a first member (Alice) and a second member (Bob).

For at least these reasons, Appellant submits that even if the teachings of *Ginzboorg et al.*, the Woo-Lam protocol, and the Otway-Rees protocol were combined, the combination would not yield the claimed invention. Accordingly, Appellant respectfully requests that the Examiner's rejection of claims 113, and its dependent claims, be reversed.

K. The rejection of claim 114 is improper because combination of *Ginzboorg et al.* with portions of the Woo-Lam and Otway-Rees protocols does not yield the claimed invention.

Although having vastly different pre-conditions and assumptions, both the Woo-Lam protocol and the Otway-Rees protocol are performed before a transaction between two parties can take place. The reason is that before these protocols are performed, the user's are not certain of each other's identity. Therefore, Appellant submits that the Otway-Rees protocol or the Woo-Lam protocol, either considered individually or in combination, do not teach or suggest anything resembling a transaction request or transaction response message as recited in claim 114. For at least these reasons, Appellant submits that even if the teachings of *Ginzboorg et al.*, the Woo-Lam protocol, and the Otway-Rees protocol were combined, the combination would not yield the claimed invention. Accordingly, Appellant respectfully requests that the Examiner's rejection of claim 114 be reversed.

L. The rejection of claim 115 is improper because combination of *Ginzboorg et al.* with portions of the Woo-Lam and Otway-Rees protocols does not yield the claimed invention.

In the Otway-Rees protocol, Trent generates one session key that is shared with both Alice and Bob. However, according to the claim, the service provider generates both a plurality of first session keys and a second session key, that are different. Thus, the combination of protocols suggested by the Examiner does not teach or suggest the generating of the different session keys, as required by the claim. Accordingly, Appellant respectfully requests that the Examiner's rejection of claim 115 be reversed.

M. Conclusion

In view of the foregoing reasons and authorities, Appellants respectfully submit that the rejection of claims 82-116 is improper and a reversal of the Examiner by the Board is required.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 50-1946 and please credit any excess fees to such deposit account.

Respectfully submitted,

Date: 12-20-05

Craig Gelfound
Registration No. 41,032

McDERMOTT, WILL & EMERY, LLP
2049 Century Park East, 34th Floor
Los Angeles, CA 90067
Telephone: (310) 277-4110
Facsimile: (310) 277-4730

APPENDIX OF CLAIMS INVOLVED IN THE APPEAL

82. A method of conducting an electronic transaction using an electronic card having a public key of a service provider, comprising:

formatting a key exchange request message at a member, the key exchange request message having a public key of the member, and at least a portion of the key exchange request message being encrypted using the service provider's public key from the electronic card;

sending the key exchange request message from the member to the service provider;

generating a session key exclusively at the service provider in response to the key exchange request message;

formatting a key exchange response message including the session key at the service provider;

sending the key exchange response message from the service provider to the member; and

using the session key to complete the transaction.

83. The method of claim 82 wherein the key exchange request message further includes a member challenge for the service provider, and the key exchange response message further includes a response to the member challenge and a service provider challenge for the member, the method further comprising formatting by the member a response to the service provider challenge and sending it to the service provider.

84. The method of claim 82 or 83 wherein the use of the session key to complete the transaction comprises:

formatting by the member a transaction request message using the session key, the transaction request message including a digital signature of the member, and sending the transaction request message to the service provider; and

formatting at the service provider, a transaction response message for the member using the session key, the transaction response including a digital signature of the service provider, and sending the transaction response message to the member.

85. The method of claim 84 wherein the transaction request message includes account information, transaction amount and transaction data, and wherein the formatting of the transaction request message by the member comprises encrypting with the session key the account information, the transaction amount and a portion of the transaction data.

86. The method of claim 84 wherein the transaction request message comprises plain text.

87. The method of claim 84 wherein the transaction request message comprises a transaction identification assigned to the member by the service provider.

88. The method of claim 84 wherein the transaction request message comprises the response to the service provider challenge.

89. The method of claim 84 wherein the transaction response message includes data encrypted with the session key.

90. The method of claim 84 wherein the transaction response message includes plain text.

91. The method of claim 84 wherein the transaction response message includes a transaction identifier assigned by the service provider to the member.

92. The method of claim 84 further comprising formatting at the member, using the session key, a transaction acknowledgment message, digitally signing by the member the transaction acknowledgment message, and sending the transaction acknowledgment message to the service provider.

93. The method of claim 92 wherein the transaction acknowledgement message includes data encrypted with the session key.

94. The method of claim 92 wherein the transaction acknowledgement message includes plain text.

95. The method of claim 92 wherein the transaction acknowledgement message includes a transaction identifier assigned to the member by the service provider.

96. A method of conducting an electronic transaction using an electronic card having a public key of a service provider, comprising:

generating a member challenge by a member;

encrypting by the member the member challenge using the service provider's public key from the electronic card to generate a first cryptogram;

formatting by the member a key exchange request message including the first cryptogram and a public key of the member;

signing digitally by the member the key exchange request message;

sending the digitally signed key exchange request message from the member to the service provider;

generating by the service provider a service provider challenge;

generating exclusively by the service provider a session key;

encrypting by the service provider the service provider challenge and the session key using the member's public key to generate a second cryptogram;

formatting by the service provider a key exchange response message including the second cryptogram and a response to the member challenge;

signing digitally by the service provider the key exchange response message;

sending the digitally signed key exchange response message to the member;

encrypting by the member a member response for the service provider challenge using the session key to generate a third cryptogram;

attaching the third cryptogram to a transaction message going from the member to the service provider;

signing digitally by the member the transaction message going from the member to the service provider; and

sending the transaction message from the member to the service provider.

97. The method of claim 96 wherein the key exchange request message and key exchange response message each comprises plain text.

98. The method of claim 96 wherein the key exchange request message comprises the member's public key encrypted with the service provider's public key.

99. The method of claim 96 wherein the generation of the second cryptogram further comprises encrypting the member challenge response as part of the second cryptogram.

100. The method of claim 96 wherein the generation of the second cryptogram further comprises encrypting a transaction identifier as part of the second cryptogram.

101. The method of claim 96 wherein the key exchange response message further includes a transaction identifier comprising plain text.

102. The method of claim 101 further comprising using the transaction identifier with a second transaction message following the transaction message and going from the member to the service provider.

103. A method of communication using an electronic card having a public key of a service provider, comprising:

formatting a first key exchange request message at a first member, the first key exchange request message having a public key of the first member, and at least a portion of the first key exchange request message being encrypted using the service provider's public key from the electronic card;

sending the first key exchange request message from the first member to a second member;

combining at a second member, a second member key exchange request message with the first member's key exchange request message and sending the combined key exchange request message, signed by the second member, to a service provider;

generating a first session key exclusively by the service provider in response to the first key exchange request message;

generating a second session key exclusively by the service provider in response to the second key exchange request message;

formatting a key exchange response message at the service provider including a first session key for the first member, signing the response message, formatting a key exchange response message including the second session key for the second member, combining the key exchange response messages into a combined key exchange response message, signing the combined key exchange response message, and sending the combined key exchange response message to the second member; and

separating at the second member, the key exchange response message for the second member from the key exchange response message for the first member, and forwarding the key exchange response message for the first member to the first member.

104. The method of claim 103 further comprising:

formatting by the first member, using the first session key, a transaction request message, signing the transaction request message, and sending the transaction request message to the second member;

formatting by the second member, using the second session key, a transaction request message;

combining by the second member, the second member transaction request message with the first member transaction request message, signing the combined transaction request message, and sending the combined transaction request message to the service provider;

formatting by the service provider, using the first session key, a transaction response message for the first member, and signing the transaction response message;

formatting by the service provider, using the second session key, a transaction response message for the second member;

combining the transaction response message for the first member with the transaction response message for the second member to form a combined transaction response message, and signing the combined transaction response message;

sending the combined transaction response message to the second member;

separating at the second member, the transaction response message for the first member from the transaction response message for the second member; and

forwarding by the second member the transaction response message for the first member to the first member.

105. The method of claim 104 further comprising:

formatting at the first member, using the first session key, an acknowledgment message, signing the acknowledgment message, and sending the acknowledgment message to a second member; and

formatting at the second member, using the second session key, an acknowledgment message, combining the second member acknowledgment message with the first member acknowledgment message to form a combined acknowledgment message, signing the combined acknowledgment message, and sending the combined acknowledgment message to the service provider.

106. The method of claim 103 wherein the first session key is different from the second session key.

107. The method of claim 103 wherein the first session key is the same as the second session key.

108. The method of claim 103 wherein the key exchange response message for the second member includes the public key of the first member, and the key exchange response message for the first member includes the public key of the second member.

109. A method of communication using an electronic card having a public key of a service provider, comprising:

formatting a first key exchange request message at a first member, the first key exchange request message having a public key of the first member, and at least a portion of the first key exchange request message being encrypted using the service provider's public key from the electronic card;

sending the first key exchange request message from the first member to at least one intermediate member coupled in series between the first member and the service provider, each of said at least one intermediate member being either a message router or a participating member;

generating, if said at least one intermediate member comprises at least one participating member, at each of the participating members a key exchange request;

receiving at the service provider a combined key exchange request message from said at least one intermediate member, the combined key exchange request message comprising the first key exchange request message and the key exchange request message generated by each of the participating members;

generating exclusively by the service provider a first session key for the first member and a participating session key for each of the participating members;

formatting at the service provider a key exchange response message including each of the first and participating session keys;

sending the key exchange response message from the service provider to said at least one intermediate member;

separating by each participating member its respective participating session key from the key exchange response message; and

sending the first session key from said at least one intermediate member to the first member.

110. The method of claim 109 further comprising:

encrypting a first transaction request message using the first session key at the first member;

sending the first transaction request message from the first member to said at least one intermediate member;

generating, if said at least one intermediate member comprises at least one participating member, at each of the participating members a transaction request message encrypted using its respective participating session key;

receiving at the service provider a combined transaction request message from said at least one intermediate member, the combined transaction request message comprising the first transaction request message and the transaction request message for each of the participating members;

formatting at the service provider a combined transaction response message comprising a transaction response message for the first member and each of the participating members;

sending the combined transaction response message from the service provider to said at least one intermediate member;

separating by each participating member its respective transaction response message from the combined transaction response message; and

sending the transaction response message for the first member from said at least one intermediate member to the first member.

111. The method of claim 109 wherein the first session key and the participating session keys are each different from one another.

112. The method of claim 109 wherein the first session key and the participating session keys are the same as each other.

113. A method of communication using an electronic card having a public key of a service provider, comprising:

formatting a key exchange request message at each of a plurality of first members, the key exchange request message for one of the first members having a public key of said one of the first members, and at least a portion of the key exchange request message for said one of the first members being encrypted using the service provider's public key from the electronic card;

sending from each of the first members its respective key exchange request message to a second member, the second member being either a message router or a participating member;

generating, if the second member is a participating member, a second key exchange request message at the second member;

combining at the second member the key exchange request message from each of the first members to form a combined key exchange request message, the combined key exchange request message further comprising the second key exchange request message if the second member is a participating member;

receiving at the service provider the combined key exchange request message from the second member;

generating exclusively by the service provider a first session key for each of the first members, and a second session key for the second member if the second member is a participating member;

formatting at the service provider a key exchange response message including each of the first and second session keys;

sending the key exchange response message from the service provider to the second member;

separating by the second member the second session key from the key exchange response message if the second member is a participating member;

separating by the second member the first session key for each of the first members from the key exchange response message; and

sending each of the first session keys to its respective first member.

114. The method of claim 113 further comprising:

encrypting a transaction request message at each of the first members using their respective first session keys;

sending from each of the first members its respective transaction request message to the second member;

generating, if the second member is a participating member, a second transaction request message at the second member and encrypting the second transaction request message with the second session key;

combining at the second member the transaction request message from each of the first members to form a combined transaction request message, the combined transaction request message further comprising the second transaction request message if the second member is a participating member;

receiving at the service provider the combined transaction request message from the second member;

generating at the service provider a transaction response message for each of the first members, and the second member if the second member is a participating member;

formatting at the service provider a combined transaction response message including the transaction response messages for each of the first members, and the second member if the second member is a participating member;

sending the combined transaction response message from the service provider to the second member;

separating by the second member its respective transaction response message from the combined transaction response message if the second member is a participating member;

separating by the second member the transaction response messages for each of the first members from the combined transaction response message; and

sending each of the transaction response messages to its respective first member.

115. The method of claim 113 wherein the first session keys and the second session key are each different from one another.

116. The method of claim 113 wherein the first session keys and the second session key are the same as each other.